

# No-iteration of unknown quantum gates

Mehdi Soleimanifar<sup>\*</sup> and Vahid Karimipour<sup>†</sup>

*Department of Physics, Sharif University of Technology, Tehran, Iran*

We propose a new no-go theorem by proving the impossibility of constructing a deterministic quantum circuit that iterates a unitary oracle by calling it only once. Different schemes are provided to bypass this result and to approximately realize the iteration. The optimal scheme is also studied. An interesting observation is that for large number of iterations, a trivial strategy like using the identity channel has the optimal performance, and preprocessing, postprocessing, or using resources like entanglement does not help at all. Intriguingly, the number of iterations, when being large enough, does not affect the performance of the proposed schemes.

PACS numbers: 03.67.-a, 03.67.Lx, 03.67.Ac

## I. INTRODUCTION

No-go theorems play a major role in quantum information science. The impossibility of perfect cloning of an unknown pure state, the *no-cloning theorem*, is one of the striking features of quantum mechanics [1]. This no-go result is fundamental to key distribution [2], quantum secret sharing [3], and quantum error correction [4]. A similar no-go theorem is valid for cloning of an *unknown quantum gate* from one to two copies [5]; that is to say, given a set of distinct states  $\bigotimes_{i=1}^m |\psi_i\rangle$  and an unknown unitary channel  $\mathcal{U}$ , it is impossible to prepare  $\bigotimes_{i=1}^m \mathcal{U}|\psi_i\rangle$  by a quantum circuit that uses  $\mathcal{U}$  only once. This result has implications in cryptographic protocols where the secret is encoded in unitary transformations instead of quantum states, e.g., an alternative version of BB84 protocol where Alice uses two orthogonal bases of unitary transformations instead of states [5].

The no-cloning of states is about the impossibility of realizing a specific transformation of *states*, while the no-cloning of gates is about a transformation of *unitary channels*. Other examples of no-go theorems on transformations of quantum channels are: The impossibility of realizing the *switch* circuit defined by  $\mathcal{Z}(\mathcal{V}, \mathcal{W}) = |0\rangle\langle 0| \otimes \mathcal{V}\mathcal{W} + |1\rangle\langle 1| \otimes \mathcal{W}\mathcal{V}$ , in which a pair of input unitary blackboxes  $\mathcal{V}$  and  $\mathcal{W}$  are connected in two different orders conditioned on the value of an input bit [6]. By generalizing the conventional quantum circuit model to bypass this no-go result, a computational advantage can be obtained [7]. Another example is the no-go theorem on controlling a unitary gate given as a blackbox discussed in [8–10], or failure of programming a quantum gate array  $\mathcal{G}$  that deterministically implements the unitary operation  $\mathcal{U}$  determined by the quantum program  $|P_U\rangle$  or strictly speaking  $\mathcal{G}(|\psi\rangle \otimes |P_U\rangle) = \mathcal{U}|\psi\rangle \otimes |P'_U\rangle$  [11].

In this paper, we introduce and investigate a new no-go theorem on *iterations of an unknown quantum gate*. The iteration of a unitary gate is widely used in quantum algorithms. Quantum search algorithms like Grover algorithm [12] or quantum random walk search algorithm [13] are based on the repetition of a unitary oracle. They use iterations of the oracle to amplify the amplitude of a desired state in a superposition of states [14]. Quantum phase estimation [15] is another algorithm in which successive iterations of a unitary gate are used to generate states appropriate for an inverse quantum Fourier transform. These algorithms are bases of other quantum computations like order finding [15], integer factorization and discrete logarithms [16] or the collision problem [17].

The question we try to answer is whether it is possible to avoid iterations of a unitary oracle using a deterministic quantum circuit. One possible scenario for doing this is that an apparatus called *gate iterator* of the  $n$ 'th order ( $n \in \mathbb{N}/\{1\}$ ), denoted by  $\text{Iter}_n$ , takes a unitary oracle  $\mathcal{U}$ , an arbitrary state  $|\psi\rangle$  and the state of the rest of the world  $|0\rangle$  as inputs, and by calling  $\mathcal{U}$  once, gives  $\mathcal{U}^n|\psi\rangle$  as the output. The state  $|0\rangle$  may also change to another state  $|0'\rangle$  at the end, see Fig. 1. In a more general scenario, the input system could be mixed and the output state be entangled with the ancillary system.

We prove that it is impossible to realize  $\text{Iter}_n$  which consists of a deterministic quantum circuit. We first consider the most general circuit for doing the iteration consists of a *preprocessing* and a *postprocessing* channel. We then show that such a procedure contradicts the linearity of quantum mechanics.

<sup>\*</sup> mehdi.soleimanifar@gmail.com

<sup>†</sup> vahid@sharif.edu

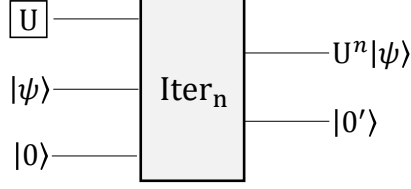


FIG. 1. In a possible scenario, the gate iterator apparatus,  $\text{Iter}_n$ , takes  $\mathcal{U}$ ,  $|\psi\rangle$  and  $|0\rangle$  as inputs and gives  $U^n|\psi\rangle$  as the output.

Although it is not possible to construct  $\text{Iter}_n$  perfectly, it is natural to ask for strategies that realize it in an approximate way. We propose such schemes and then, by using the notion of *fidelity* as a figure of merit, we investigate their performance and how it scales with the number of iterations  $n$ , and the dimensionality of the state  $d$ . We also address the problem of finding the optimal iterator. We show that the optimal fidelity is the answer of a semidefinite programming. We solve this problem numerically for  $d = 2, 3$ , see Fig. 6.

As we will see, the approximate realization of a gate iterator has interesting characteristics. We show that in all strategies, including the optimal, by increasing the dimension of the system  $d$ , the fidelity decreases. Intriguingly, the fidelity reaches a constant value by increasing  $n$ , so when we are allowed to query a unitary oracle only once, there is no difference in quality of high-order imperfect iterations of that. Another interesting observation is that when  $n > d$ , a trivial strategy like approximating  $U^n$  by  $\mathcal{U}$  or even by the identity channel has the optimal performance, and preprocessing, postprocessing, or using resources like entanglement does not help at all. These results are depicted in Fig. 3, 4 and 6.

An anticipated result of our no-go theorem is that when the oracle is completely unknown, the only way to perform iterations of that, seems to be calling the oracle each time and give the state to that and do this repeatedly. For a large number of iterations, this makes the algorithm inefficient. In fact, one way of comparing the complexity of different algorithms is to count the necessary number of querying within the program [18].

The rest of the paper is organized as follows: In the next section, notations and some basic definitions are presented, and a convenient figure of merit is introduced to measure how good a quantum circuit approximates a given unitary gate. In Sec. III, we prove the no-iteration theorem for an arbitrary order  $n$ . The fidelity and details of the *random guess* and *measure-and-prepare* strategies are discussed in Sec. V and IV. Then, two trivial but important methods are introduced in Sec. VI, and the optimum fidelity is obtained numerically in Sec. VII. Finally, we conclude the paper in Sec. VIII.

## II. NOTATIONS AND CONVENTIONS

In this section, we gather some well-known facts which we will frequently use in the sequel. We denote the complex  $d$ -dimensional Hilbert space by  $\mathcal{H}_d$ , and the linear space of operators acting on it by  $L(\mathcal{H}_d)$  and the set of density matrices by  $D(\mathcal{H}_d)$ . A basis for  $\mathcal{H}_d$  is denoted by  $\{|j\rangle : j = 1, 2, \dots, n\}$  and any linear operator  $V$  in  $L(\mathcal{H}_d)$  is expanded as  $V = \sum_{j,k} V_{jk} |j\rangle\langle k|$ . A correspondence between this operator and a vector  $|V\rangle\rangle \in \mathcal{H}_d \otimes \mathcal{H}_d$  can be established by defining

$$|V\rangle\rangle := \frac{1}{\sqrt{d}} \sum_{j,k} V_{jk} |j\rangle|k\rangle, \quad (1)$$

where  $|V\rangle\rangle$  is called the *vectorized form* of the operator  $V$ . Therefore, the maximally entangled state  $|\phi^+\rangle := \frac{1}{\sqrt{d}} \sum_j |j\rangle|j\rangle$  is the vectorized form of the identity operator, i.e.,  $|\phi^+\rangle = |\mathbb{1}\rangle\rangle$ . The inner product between two operators  $A$  and  $B$  defined as  $\text{Tr}(A^\dagger B)$  can equally be written as the ordinary vector product of their vectorized form, that is  $\text{Tr}(A^\dagger B) = \langle\langle A|B\rangle\rangle$ . Finally, we note that a vector  $|V\rangle\rangle$  can be prepared by performing  $V$  on the maximally entangled state  $|\mathbb{1}\rangle\rangle$ :

$$|V\rangle\rangle = V \otimes \mathbb{1} |\mathbb{1}\rangle\rangle. \quad (2)$$

The Choi operator  $R_{\mathcal{T}}$  associated with a quantum channel  $\mathcal{T} : D(\mathcal{H}_d) \rightarrow D(\mathcal{K}_d)$  is defined on  $\mathcal{K}_d \otimes \mathcal{H}_d$  by

$$R_{\mathcal{T}} := (\mathcal{T} \otimes \mathcal{I}) (|\mathbb{1}\rangle\rangle\langle\langle\mathbb{1}|), \quad (3)$$

where  $\mathcal{I}$  is the identity channel. Obviously, we have  $R_{\mathcal{I}} := |\mathbb{1}\rangle\langle\mathbb{1}|$ , that is to say, the Choi operator of the identity channel is the Bell state.

A unitary quantum channel (quantum gate)  $\mathcal{U}$  is defined as

$$\mathcal{U}(\rho) := U\rho U^\dagger, \quad (4)$$

that according to Eq. (2), its Choi operator is the pure state  $R_{\mathcal{U}} = |U\rangle\langle U|$ .

When we want to evaluate the performance of a process  $\mathcal{E}$  that approximates a gate  $\mathcal{U}$ , we need to introduce a figure of merit. The fidelity between two channels  $\mathcal{G}$  and  $\mathcal{E}$  is defined to be the state fidelity between the Choi operators of these channels [19]:

$$\mathcal{F}(\mathcal{G}, \mathcal{E}) := \left( \text{Tr} \left( \sqrt{\sqrt{R_{\mathcal{G}}} R_{\mathcal{E}}} \sqrt{R_{\mathcal{G}}} \right) \right)^2, \quad (5)$$

which reduces to the following when one of them is a unitary channel of the form (4)

$$\mathcal{F}(\mathcal{U}, \mathcal{E}) = \langle\langle U | R_{\mathcal{E}} | U \rangle\rangle. \quad (6)$$

Now, we assume that instead of a single gate, a specific set of gates  $S$ , consists of a finite or infinite collection of unitary gates, are to be approximated with a process  $\mathcal{E}$ , and each gate  $U \in S$  occurs with probability  $P(U)$ . The input of  $\mathcal{E}$  is a given  $U \in S$  and the output is  $\mathcal{E}_U$ . Then, a figure of merit that determines the performance of process  $\mathcal{E}$  is given by:

$$F(\mathcal{E}) := \int dU P(U) \mathcal{F}(\mathcal{U}, \mathcal{E}_U). \quad (7)$$

Here,  $dU$  is an invariant Haar measure, that is  $d(UV) = d(VU) = dU$ ,  $\forall V \in \mathbb{U}(d)$ . When  $S$  is the unitary group  $\mathbb{U}(d)$ , and gates are chosen uniformly,  $P(U) = 1$ ,  $\forall U \in \mathbb{U}(d)$ .

### III. NO-ITERATION OF UNKNOWN QUANTUM GATES

We now prove the impossibility of implementing  $\text{Iter}_n$ . We call this no-go result, the *no-iteration of unknown quantum gates* and provide two proofs for that. One, for the case that the output states are product states, is based on the linearity of the quantum circuit that implements  $\text{Iter}_n$ , and a more general proof, available in Appendix A, is a corollary of a lower bound on the performance of quantum search algorithms. As another confirmation for the validity of this theorem, the optimum fidelity for approximating  $\text{Iter}_n$  is obtained numerically for  $d = 2, 3$  in Sec. VII, and as expected, it is less than 1.

**Theorem 1.** *The universal deterministic gate iterator of order  $n$ ,  $\text{Iter}_n$ , cannot be implemented perfectly.*

**Proof.** The most general quantum circuit that uses a single copy of  $\mathcal{U}$  to implement  $\mathcal{U}^n$  is depicted in Fig. 2 [20, 21].  $\mathcal{A}_n$  and  $\mathcal{B}_n$  are preprocessing and postprocessing gates respectively, and  $|0\rangle$  shows the ancillary system. This circuit transforms inputs to  $B_n(U \otimes \mathbb{1}) A_n |\psi\rangle \otimes |0\rangle$ . In this proof, it is assumed that input states are pure and output states are product states (this is relaxed in the alternate proof, see Appendix A), so the output is of the form  $U^n |\psi\rangle \otimes |a_U\rangle$  where  $|a_U\rangle$  is the output ancillary system that possibly depends on  $U$ .

To prove the theorem, it must be shown that no quantum gates  $\mathcal{A}_n$  and  $\mathcal{B}_n$  can be found such that for all unitary gates  $\mathcal{U}$

$$B_n(U \otimes \mathbb{1}) A_n |\psi\rangle \otimes |0\rangle = U^n |\psi\rangle \otimes |a_U\rangle. \quad (8)$$

This can be seen by noticing the linearity of the LHS of Eq. (8) with respect to  $U$ , while the RHS seems not to be so. In order to show that this is not possible, we use the linearity of quantum mechanics. To proceed, we need two unitary operators so that their linear combinations is also unitary. We take these operators to be

$\mathbb{1}$  and  $\Omega = \sum_{k=0}^{d-1} |k\rangle\langle d-k-1| = \begin{pmatrix} & & 1 \\ & \ddots & \\ 1 & & \end{pmatrix}$ . Note that  $\Omega$  is both unitary and Hermitian, so  $\Omega^2 = \mathbb{1}$ , which makes  $U := \cos \theta \mathbb{1} + i \sin \theta \Omega$ , also unitary for every  $\theta$ . Therefore, we should have

$$\begin{aligned} B_n(\mathbb{1} \otimes \mathbb{1}) A_n |\psi\rangle \otimes |0\rangle &= \mathbb{1} |\psi\rangle \otimes |a_{\mathbb{1}}\rangle \\ B_n(\Omega \otimes \mathbb{1}) A_n |\psi\rangle \otimes |0\rangle &= \Omega^n |\psi\rangle \otimes |a_{\Omega}\rangle \\ B_n((\cos \theta \mathbb{1} + i \sin \theta \Omega) \otimes \mathbb{1}) A_n |\psi\rangle \otimes |0\rangle &= (\cos \theta \mathbb{1} + i \sin \theta \Omega)^n |\psi\rangle \otimes |a_{\theta}\rangle, \end{aligned} \quad (9)$$

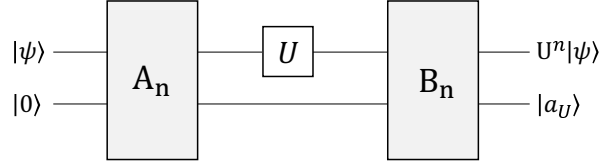


FIG. 2. The Stinespring realization of the quantum circuit of  $\text{Iter}_n$

where  $|a_\theta\rangle$  stands for  $|a_{\cos\theta\mathbb{1}+i\sin\theta\Omega}\rangle$ . Using the first two equations in the LHS of the third, we find

$$\cos\theta \mathbb{1}|\psi\rangle \otimes |a_{\mathbb{1}}\rangle + i\sin\theta \Omega^n|\psi\rangle \otimes |a_\Omega\rangle = (\cos n\theta \mathbb{1} + i\sin n\theta \Omega)|\psi\rangle \otimes |a_\theta\rangle. \quad (10)$$

By looking at a specific entry of the first factor, we get

$$\cos\theta \langle 0|\mathbb{1}|d-1\rangle |a_{\mathbb{1}}\rangle + i\sin\theta \langle 0|\Omega^n|d-1\rangle |a_\Omega\rangle = \langle 0|(\cos n\theta \mathbb{1} + i\sin n\theta \Omega)|d-1\rangle |a_\theta\rangle, \quad (11)$$

but since  $\Omega^n = \Omega$  for odd  $n$ , and  $\Omega^n = \mathbb{1}$  for even  $n$ , and  $\langle 0|\mathbb{1}|d-1\rangle = 0$ ,  $\langle 0|\Omega|d-1\rangle = 1$ , we find

$$\sin n\theta = \begin{cases} 0 & n \text{ even} \\ \pm \sin\theta & n \text{ odd} \end{cases} \quad (12)$$

that cannot be satisfied for arbitrary  $\theta$ . □

Although it is impossible to perfectly iterate an unknown gate in  $\mathbb{U}(d)$ , if a unitary is randomly picked from a set of *jointly perfectly discriminable unitaries*, then clearly it is possible to iterate it. Whether or not the set of perfectly discriminable unitaries is the only set with this property, is an open question and remains for further investigation [22].

In the forthcoming sections, we explore different schemes that not perfectly but approximately bypass the introduced no-go result.

#### IV. THE RANDOM GUESS STRATEGY

In this section, we investigate the random guess strategy in which the input gate is discarded and iterations of a randomly chosen unitary channel are applied to the input state. The random gate is chosen according to a probability distribution induced by normalized Haar measure on  $\mathbb{U}(d)$ . Therefore, it can be expressed with the following process

$$\mathcal{J}_n(\rho) = \int dV V^n \rho V^{n\dagger}. \quad (13)$$

The motivation for studying this rather simple or blind strategy is that it plays an important role for understanding and comparing the performance of other strategies discussed in the following sections.

Let us begin by a theorem on the fidelity of this process:

**Theorem 2.** *The fidelity of the random guess strategy is*

$$F_{\text{rand},n} = p_n^2 + \frac{1-p_n^2}{d^2}, \quad (14)$$

where

$$p_n = \frac{\min(n,d)-1}{d^2-1}. \quad (15)$$

Before we give the proof of this theorem, we need two lemmas.

**Lemma IV.1.** *For all self-adjoint matrices  $M \in L(\mathcal{H}_d)$*

$$\mathcal{J}_n(M) := \int dU U^n M U^{n\dagger} = p_n M + (1-p_n) \text{Tr}(M) \frac{\mathbb{1}}{d}, \quad (16)$$

where the integration is with respect to the normalized Haar measure on  $\mathbb{U}(d)$ , and  $p_n$  is the same as Eq. (15).

**Proof of Lemma.** Let  $\mathcal{E}$  be any quantum channel. The *twirled transformation* associated with  $\mathcal{E}$  is defined as

$$\tilde{\mathcal{E}}(M) := \int dV V \mathcal{E}(V^\dagger M V) V^\dagger. \quad (17)$$

It is shown in in [23], that the twirled transformation acts like a depolarizing channel with parameter  $p_{n,\mathcal{E}}$  that depends on the original channel  $\mathcal{E}$ :

$$\tilde{\mathcal{E}}(M) = p_{n,\mathcal{E}} M + (1 - p_{n,\mathcal{E}}) \text{Tr}(M) \frac{\mathbb{1}}{d}. \quad (18)$$

For the specific channel  $\mathcal{J}_n$ , the twirled channel  $\tilde{\mathcal{J}}_n$  equals  $\mathcal{J}_n$  itself. To see this, we note that

$$\tilde{\mathcal{J}}_n(\rho) = \int dV \int dU (V U^n V^\dagger) \rho (V U^{n\dagger} V^\dagger). \quad (19)$$

By defining  $W := V U V^\dagger$  and using right and left invariance of Haar measure, we find

$$\tilde{\mathcal{J}}_n(\rho) = \int dV \int dW W^n \rho W^{n\dagger} = \int dV \mathcal{J}_n(\rho) = \mathcal{J}_n(\rho), \quad (20)$$

where we have used the normalization  $\int dV = \mathbb{1}$ . It remains to determine the value of the parameter  $p_n := p_{n,\mathcal{J}_n}$ . To do this, we enact the channel  $\mathcal{J}_n$  on the matrix  $|i\rangle\langle j|$  to obtain

$$\int dU U^n |i\rangle\langle j| U^{n\dagger} = p_n |i\rangle\langle j| + (1 - p_n) \delta_{ij} \frac{\mathbb{1}}{d}. \quad (21)$$

Multiplying both sides by  $\langle i|$  and  $|j\rangle$  and summing over  $i$  and  $j$ , we find

$$\int dU |\text{Tr}(U^n)|^2 = p_n d^2 + (1 - p_n). \quad (22)$$

Using theorem 2.1 of [24], according to which  $\int dU |\text{Tr}(U^n)|^2 = \min(n, d)$ , we finally find the value of  $p_n$ :

$$p_n = \frac{\min(n, d) - 1}{d^2 - 1}. \quad (23)$$

This completes the proof.  $\square$

**Corollary 1.** For all self-adjoint matrices  $M \in L(\mathcal{H}_d^{(1)} \otimes \mathcal{H}_d^{(2)})$

$$\begin{aligned} \mathcal{K}_n(M) &:= \int dU (U^n \otimes \mathbb{1}) M (U^{n\dagger} \otimes \mathbb{1}) \\ &= p_n M + (1 - p_n) \frac{\mathbb{1} \otimes \text{Tr}_1(M)}{d}. \end{aligned} \quad (24)$$

**Corollary 2.** By substituting  $M = |\mathbb{1}\rangle\langle\mathbb{1}|$  in Eq. (24), we get

$$\int dU |U^n\rangle\langle U^n| = p_n |\mathbb{1}\rangle\langle\mathbb{1}| + (1 - p_n) \frac{\mathbb{1}}{d^2}. \quad (25)$$

**Proof of Theorem 2.** According to Eq. (6), approximating the iteration of a given gate  $\mathcal{U}$  with the iteration of a Haar-distributed random gate  $\mathcal{V}$  has the fidelity  $\mathcal{F}(\mathcal{U}^n, \mathcal{V}^n) = |\langle U^n | V^n \rangle|^2$ , so its expected value is

$$\mathbb{E}[\mathcal{F}(\mathcal{U}^n, \mathcal{V}^n)] = \langle U^n | \left( \int dU |V^n\rangle\langle V^n| \right) | U^n \rangle \quad (26)$$

$$= p_n |\langle U^n | \mathbb{1} \rangle|^2 + (1 - p_n) \frac{1}{d^2}, \quad (27)$$

where the second equality follows from Eq. (25). The fidelity of the random guess strategy can be obtained by taking the average over all  $\mathcal{U}$ 's:

$$F_{rand,n} = \int dU \mathbb{E}[\mathcal{F}(\mathcal{U}^n, \mathcal{V}^n)] \quad (28)$$

$$= p_n \int dU |\langle U^n | \mathbb{1} \rangle|^2 + (1 - p_n) \frac{1}{d^2}. \quad (29)$$

Again, the integral is simplified using Eq. (25):

$$F_{rand,n} = p_n^2 + \frac{1 - p_n^2}{d^2}. \quad (30)$$

$\square$

As stated in Theorem 2 and depicted in Fig. 3, the fidelity of the random guess decreases quadratically with growth of the dimension  $d$ , but less intuitively is a kind of *phase transition* occurs at  $n = d$ : the fidelity increases with growth of  $n$  for  $n < d$ , and reaches a constant value for  $n \geq d$ . The random guess is not the only scheme with such phase transition, and as we shall see in next sections, this is a characteristic of all of our approximating strategies. The same phenomena is observed in a similar context when dealing with the joint distribution  $f(\theta_1, \dots, \theta_d)$  of eigenvalues  $\{e^{i\theta_j}\}_{j=1}^d$  of a Haar-distributed unitary matrix in  $\mathbb{U}(d)$  [25], that is

$$f(\theta_1, \dots, \theta_d) = \frac{1}{(2\pi)^d d!} \prod_{j < k} |e^{i\theta_j} - e^{i\theta_k}|^2, \quad (31)$$

so when  $\theta_j \rightarrow \theta_k$ ,  $f \rightarrow 0$ , and eigenvalues somehow repel each other. To see this more intuitively, consider  $d$  identically charged particles confined to move on the unit circle with Coulomb interaction between them. Their associated Gibbs distribution is

$$f(\theta_1, \dots, \theta_d) = \frac{1}{(2\pi)^d d!} e^{-\beta H(\theta_1, \dots, \theta_d)}, \quad (32)$$

with the Hamiltonian  $H = -\sum_{j < k} \log |e^{i\theta_j} - e^{i\theta_k}|$  and  $\beta = 2$ . This is the same distribution as in Eq. (31) and the repulsion of eigenvalues comes to have a clear physical meaning, and is similar to the repulsion between particles in the ordinary Coulomb gas.

When the joint distribution of eigenvalues of higher powers is considered, a phase transition occurs, and for  $n \geq d$ , the eigenvalues of  $U^n$  are exactly distributed as  $d$  points chosen independently and uniformly on the unit circle [26]. Thus, the eigenvalues that seem to have an ordered structure and are very neatly spaced for  $n = 1$  have no structure for  $n \geq d$ .

To see the connection of this result to the fidelity of the random guess, notice that from the proof of Lemma IV.1, the parameter  $p_n$  in Eq. (15) is

$$p_n = \frac{\int dU |\text{Tr}(U^n)|^2 - 1}{d^2 - 1}, \quad (33)$$

but  $\int dU |\text{Tr}(U^n)|^2$  depends on the joint distribution of eigenvalues of  $U^n$ . For  $n \geq d$ , this distribution remains the same and  $\int dU |\text{Tr}(U^n)|^2 = d$ , so  $p_n$  and fidelity also remain constant.

Finally, we prove that there exists a depolarizing channel whose fidelity equals the fidelity of the random guess and may be considered as an implementation of that.

**Theorem 3.** *The fidelity of the random guess strategy for approximating the  $n$ 'th iteration of a given unknown unitary  $\mathcal{U}$  is equal to the fidelity of the following depolarizing channel*

$$\begin{aligned} \mathcal{J}_n(\rho) &= \int dV V^n \rho V^{n\dagger} \\ &= p_n \rho + (1 - p_n) \frac{\mathbb{1}}{d}, \end{aligned} \quad (34)$$

with  $p_n = \frac{\min(n, d) - 1}{d^2 - 1}$ , the same as in Eq. (15).

**Proof.** Consider the quantum channel

$$\mathcal{J}_n(\rho) = \int dV V^n \rho V^{n\dagger}, \quad (35)$$

with  $V^n$  as its Kraus operators. The Choi operator of this channel is

$$R_{\mathcal{J}_n} = \int dV |V^n\rangle\langle V^n|, \quad (36)$$

so the fidelity of  $\mathcal{J}_n$  is

$$\begin{aligned} F(\mathcal{J}_n) &= \int dU \langle U^n | R_{\mathcal{J}_n} | U^n \rangle \\ &= \int dU \int dV |\langle U^n | V^n \rangle|^2, \end{aligned} \quad (37)$$

which is exactly the same as Eq. (28), so

$$F(\mathcal{J}_n) = F_{rand,n}. \quad (38)$$

It is also clear from Lemma IV.1 that  $\mathcal{J}_n$  is a polarizing channel

$$\mathcal{J}_n(\rho) = p_n \rho + (1 - p_n) \frac{\mathbb{1}}{d}, \quad (39)$$

with  $p_n$  as in Eq. (15).  $\square$

## V. THE ESTIMATION STRATEGY

In the previous scheme, we blindly iterated a random gate and found its fidelity. We now discuss a more prepared and discriminating strategy in which we use more resources. Namely, we estimate the given unitary blackbox and based on the result of the estimation, we choose a gate and perform its iteration on the input state.

To make things clear, we can compare it with the random guess circuit that is described by the channel  $\mathcal{J}_n(\rho) = \int dV V^n \rho V^{n\dagger}$ , Eq. (13).  $\mathcal{J}_n(\rho)$  is the average of all states  $V^n \rho V^{n\dagger}$ , and each unitary gate  $V$  has the same weight in it. We can use estimation results to give higher weights to more preferable gates. Let us denote the weight of unitary gate  $V$  by  $\omega_V$ , so the action of our approximate gate iterator is to take  $\rho$  and gives  $\int dV \omega_V V^n \rho V^{n\dagger}$  as the output. As much as these weights are decided correctly, our circuit has higher fidelity than that of the random guess and approximates  $\text{Iter}_n$  better.

One idea for obtaining reasonable weights  $\omega_V$  from a unitary channel with a single try is to encode the effect of the channel into a maximally entangled state and then perform a measurement on the state, the *measure-and-prepare* method [27]. To see how this works, we first notice that according to Corollary 2

$$\int dV |V\rangle\langle V| = \frac{\mathbb{1}}{d}, \quad (40)$$

so the set of operators  $d |V\rangle\langle V|$  provides bases for a non-orthogonal measurement. On the other hand, the state  $|U\rangle$  can be prepared by a single use of  $\mathcal{U}$ , Eq. (2). Obviously, this measurement cannot perfectly discriminate  $|U\rangle$  from other states, and after the measurement, a vector  $|V\rangle$  is obtained with probability density  $d^2 |\langle V|U\rangle|^2$ . Thus, the output state is a weighted mean of states  $V^n \rho V^{n\dagger}$  with  $\omega_V = d^2 |\langle V|U\rangle|^2$ .

As depicted in Fig. 2, the circuit may include a preprocessing unit ( $\mathcal{A}_n$ ) for preparing necessary states for estimation of  $\mathcal{U}$ , and a postprocessing unit ( $\mathcal{B}_n$ ) for performing the measurement and preparing the output state based on the estimation. Let the input state on which the iteration is performed be  $\rho$  and the ancillary system be a bipartite state  $|00\rangle\langle 00|$ . The preprocessing channel  $\mathcal{A}_n$ , prepares a maximally entangled state  $|\mathbb{1}\rangle\langle\mathbb{1}|$  from the ancillary system and swaps that with  $\rho$ , so that the input state remains unchanged until the estimation results are ready. In other words,

$$\mathcal{A}_n(\rho \otimes |00\rangle\langle 00|) = |\mathbb{1}\rangle\langle\mathbb{1}| \otimes \rho. \quad (41)$$

Then,  $\mathcal{U} \otimes \mathcal{I}$  acts on the entangled ancillary system and state  $|U\rangle\langle U|$  is prepared. In channel  $\mathcal{B}_n$ , according to the results of the measurement of  $|U\rangle\langle U|$ , unitary gates are performed on  $\rho$ , so the output is

$$\mathcal{B}_n(|U\rangle\langle U| \otimes \rho) = \int dV (d^2 |\langle V|U\rangle|^2) |V\rangle\langle V| \otimes V^n \rho V^{n\dagger}. \quad (42)$$

The action of the whole circuit on  $\rho$  is obtained by tracing the output of  $\mathcal{B}_n$  over the ancillary system:

$$\begin{aligned} \mathcal{D}_{n,\mathcal{U}}(\rho) &:= \text{Tr}_a(\mathcal{B}_n(|U\rangle\langle U| \otimes \rho)) \\ &= d^2 \int dV |\langle V|U\rangle|^2 V^n \rho V^{n\dagger}. \end{aligned} \quad (43)$$

**Theorem 4.** *The fidelity of this strategy is*

$$F_{est,n} = d^2 \text{Tr}(M_n^2), \quad (44)$$

with

$$M_n := \int dU |U\rangle\langle U| \otimes |U^n\rangle\langle U^n|. \quad (45)$$



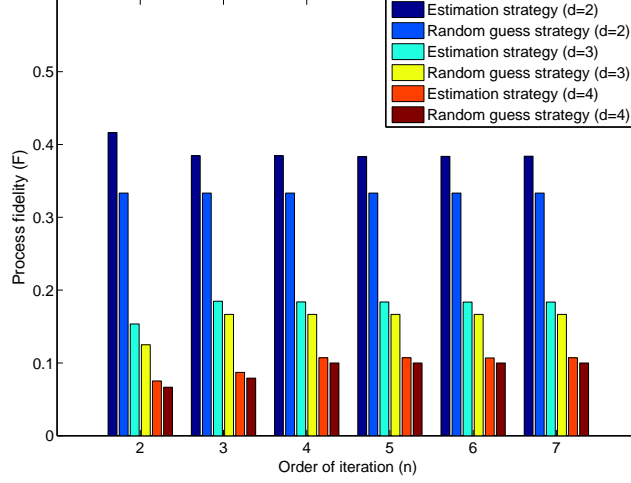


FIG. 3. Fidelity of the random guess and the estimation strategies for various orders of iteration in dimensions  $d = 2, 3$  and 4. The advantage of estimation strategy over random guess is clear. It is also seen that this advantage tends to decrease with increasing the dimension  $d$ .

**Proof.** The Choi operator associated with the map  $\mathcal{D}_{n,\mathcal{U}}$  is

$$R_{\mathcal{D}_{n,\mathcal{U}}} = d^2 \langle\langle U | \left( \int dV |V\rangle\langle V| \otimes |V^n\rangle\langle V^n| \right) | U \rangle\rangle. \quad (46)$$

The fidelity of this strategy is  $F_{est,n} = \int dU \text{Tr}(R_{\mathcal{D}_{n,\mathcal{U}}} R_{\mathcal{U}^n})$ . By replacing  $R_{\mathcal{U}^n} = |U^n\rangle\langle U^n|$ , it is immediate to get Eq. (44).  $\square$

The matrix  $M_n$  can be calculated numerically using Monte Carlo method. One approach is to generate Haar-distributed random unitary matrices in  $\mathbb{U}(d)$ . Then, the integral in Eq. (44) can be approximated by averaging the integrand over these random matrices. A simple algorithm exists for uniform generation of random matrices [28]. The idea is to generate a matrix  $Z$  with *QR-decomposition*

$$Z = QR, \quad (47)$$

where  $Q$  is unitary and  $R$  is upper-triangular and invertible. Let  $D$  be the diagonalization of  $R$  whose entries are divided by their absolute value, then it turns out that if entries of  $Z$  are *i.i.d* standard complex normal random variables, the matrix  $U = QD$  is distributed according to Haar measure [28].

The fidelity of the estimation strategy for different iteration orders is depicted in Fig. 3. It can be seen that by increasing the dimension of the input system, fidelity of the proposed circuit decreases and performance of this circuit tends to that of the random guess method. Similar to the case of the random guess, the fidelity of this circuit reaches a constant value and remains the same for higher order iterations.

Note that in the estimation strategy we could have replaced the measurement in the over-complete basis in Eq. (40), by a measurement over an orthonormal basis

$$\begin{aligned} \langle\langle U_j | U_k \rangle\rangle &= \text{Tr}(U_j^\dagger U_k) = 0 \quad \forall j, k \in \{1, \dots, d^2\}, j \neq k, \\ \sum_{j=1}^{d^2} |U_j\rangle\langle U_j| &= \mathbf{1}. \end{aligned} \quad (48)$$

which is a basis of jointly perfectly discriminable gates. In this case, the quantum channel (43) would have been replaced by

$$\tilde{\mathcal{D}}_{n,\mathcal{U}}(\rho) = \sum_{j=1}^{d^2} |\langle\langle U_j | U \rangle\rangle|^2 U_j^n \rho U_j^{n\dagger}. \quad (49)$$

However, as we will show in the next section, none of these two kinds of estimation are optimal. The same is true in the case of cloning of unitary gates [5], where  $F_{est}$  is even worse than  $F_{rand}$  for  $d > 2$ . However, for  $n = -1$ , i.e, when the unknown gate is to be inverted, the estimation strategy is the optimal scheme [29].



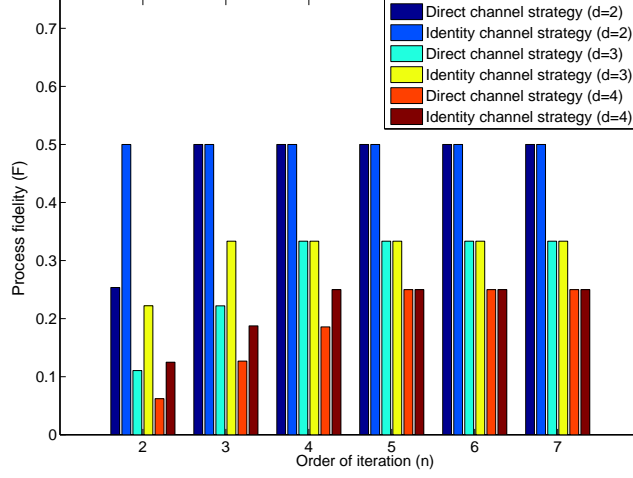


FIG. 4. Fidelity of the identity and direct channel strategies. Both schemes have equal performances for  $n > d$ , and, in fact, they achieve the optimum fidelity in this case.

## VI. THE IDENTITY AND DIRECT CHANNELS STRATEGIES

An apparently trivial strategy, called the *identity channel strategy*, is to take the identity channel as an approximation of  $\text{Iter}_n$ , i.e., to neglect the given gate  $\mathcal{U}$ , and to put the input state  $\rho$  directly in the output. To see why this approximation is *reasonable*, we note that by using Eq. (6) and Corollary 2, we get

$$\int dU \mathcal{F}(\mathcal{V}, \mathcal{U}^n) = p_n \|\langle V | \mathbb{1} \rangle\|^2 + \frac{1 - p_n}{d^2}, \quad (50)$$

which immediately gives

$$\max_{V \in \mathbb{U}(d)} \int dU \mathcal{F}(\mathcal{V}, \mathcal{U}^n) = \mathcal{F}(\mathbb{1}, \mathcal{U}^n) \quad (51)$$

so on average, the identity channel has the maximum similarity to all  $\mathcal{U}^n$ 's, and in this sense, it is a reasonable approximation of  $\mathcal{U}^n$ .

The fidelity of this channel is obtained by replacing  $\mathcal{V}$  with  $\mathbb{1}$  in Eq. (50), that gives:

**Theorem 5.** *The fidelity of the identity channel  $F_{iden,n}$  is*

$$\begin{aligned} F_{iden,n} &= \int dU \mathcal{F}(\mathbb{1}, \mathcal{U}^n) \\ &= p_n + \frac{1 - p_n}{d^2}. \end{aligned} \quad (52)$$

where  $p_n$  is given by Eq. (15).

As it can be seen in Fig. 4, the performance of this process is better than the estimation method, and for  $n \geq d$ ,  $F_{iden,n} = \frac{1}{d}$ . In fact, we will see in the next section that this channel achieves the optimum fidelity in certain cases.

The *direct channel strategy* is another trivial method with the similar performance for high enough orders  $n$ . In this case,  $\mathcal{U}^n$  is approximated by  $\mathcal{U}$  and the given gate is performed *directly* on the input state by replacing  $\mathcal{A}_n$  and  $\mathcal{B}_n$  with identity channels. Numerical results for this scheme is depicted in Fig. 4. Note that the same phase transition as in case of the estimation and random guess strategies occurs.

## VII. OPTIMUM FIDELITY

The most general form of the quantum circuit of  $\text{Iter}_n$  may be described by concatenation of different unitary channels and some ancillary systems, namely, the Stinespring realization shown in Fig. 2. Therefore, one way to find

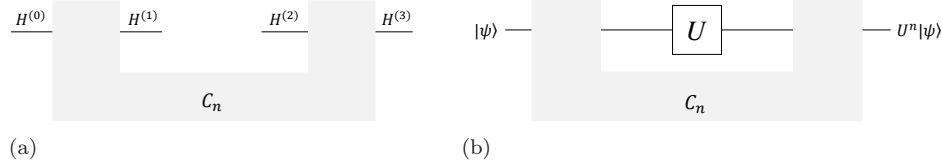


FIG. 5. (a) The channel  $\mathcal{C}_n$  with one open slot is a replacement for the Stinespring realization shown in Fig. 2, (b) the unitary gate is inserted into the slot to realize  $\text{Iter}_n$ .

the optimal process that faithfully realizes  $\text{Iter}_n$  is to maximize the fidelity over all quantum channels  $\mathcal{A}_n$  and  $\mathcal{B}_n$ . This is not the only way, and in fact, a more suitable way to describe  $\text{Iter}_n$  exists: the quantum comb notion [21].

In this method, instead of considering separate channels  $\mathcal{A}_n$  and  $\mathcal{B}_n$ , they are merged and replaced with a channel  $\mathcal{C}_n$  from  $D(\mathcal{H}^{(0)}) \otimes D(\mathcal{H}^{(2)})$  to  $D(\mathcal{H}^{(1)}) \otimes D(\mathcal{H}^{(3)})$ , see Fig. 5a. This channel has an open slot in which the given unitary gate  $\mathcal{U}$  is inserted and the  $n$ 'th iteration of  $\mathcal{U}$  is realized, Fig 5b.

In the circuit shown in Fig. 5b, the processing of information is from left to right as time passes, and the outputs may depend on the previous but not the later times inputs. Thus, not every quantum channel from  $D(\mathcal{H}^{(0)}) \otimes D(\mathcal{H}^{(2)})$  to  $D(\mathcal{H}^{(1)}) \otimes D(\mathcal{H}^{(3)})$  can be realized with such a circuit, and they need to meet additional *causality constraints*.

The *quantum comb*  $R_{\mathcal{C}_n}$  is defined as the Choi operator associated with  $\mathcal{C}_n$  acting on  $D(\mathcal{H}^{(1)}) \otimes D(\mathcal{H}^{(3)}) \otimes D(\mathcal{H}^{(0)}) \otimes D(\mathcal{H}^{(2)})$ . As it is proven in [21], the causality constraint is equivalent to the following set of linear constraints on the quantum comb  $R_{\mathcal{C}_n}$

$$\begin{aligned} \text{Tr}_3(R_{\mathcal{C}_n}) &= \frac{\mathbb{1}_2}{d} \otimes R_{\mathcal{C}_n}^{(1)} \\ \text{Tr}_1(R_{\mathcal{C}_n}^{(1)}) &= \frac{\mathbb{1}_0}{d}, \end{aligned} \quad (53)$$

where  $\text{Tr}_i$  means the partial trace over  $\mathcal{H}^{(i)}$  and  $R_{\mathcal{C}}^{(1)}$  is a Choi operator on  $\mathcal{H}^{(1)} \otimes \mathcal{H}^{(0)}$ , and subscripts of operators represent the related Hilbert space of them.

The benefit of using the quantum comb notion is clearly seen when the composition of  $\mathcal{C}_n$  with the unitary gate  $\mathcal{U}$ , denoted by  $\mathcal{C}_n \star \mathcal{U}$ , is to be described, Fig. 5b. It can be proven that (see Ref. [21]) the Choi operator of the channel  $\mathcal{C}_n \star \mathcal{U}$  is :

$$R_{\mathcal{C}_n \star \mathcal{U}} = d^2 \langle\langle U_{21}^* | R_{\mathcal{C}_n} | U_{21}^* \rangle\rangle, \quad (54)$$

where  $R_{\mathcal{C}_n \star \mathcal{U}} \in L(\mathcal{H}^{(3)} \otimes \mathcal{H}^{(0)})$  and  $U^*$  is the conjugate complex of  $U$ . The subscripts 21 in  $|U_{21}^*\rangle\rangle$  denotes the domain and image Hilbert spaces of the operator  $U$ . Thus, the fidelity (Eq. (7)) is

$$\begin{aligned} F(\mathcal{C}_n) &= \int dU \text{Tr}(d^2 \langle\langle U_{21}^* | R_{\mathcal{C}_n} | U_{21}^* \rangle\rangle |U_{30}^n\rangle\rangle \langle\langle U_{30}^n|) \\ &= \text{Tr}(d^2 R_{\mathcal{C}_n} \int dU |U_{30}^n\rangle\rangle \langle\langle U_{30}^n| \otimes |U_{21}^*\rangle\rangle \langle\langle U_{21}^*|). \end{aligned} \quad (55)$$

Let  $\tilde{M}_n := d^2 \int dU |U_{30}^n\rangle\rangle \langle\langle U_{30}^n| \otimes |U_{21}^*\rangle\rangle \langle\langle U_{21}^*|$ , then

$$F(\mathcal{C}_n) = \text{Tr}(R_{\mathcal{C}_n} \tilde{M}_n). \quad (56)$$

Therefore, to find optimal strategies for realizing  $\text{Iter}_n$ , the following optimization problem should be solved:

$$\begin{aligned} &\max_{R_{\mathcal{C}_n}} \text{Tr}(R_{\mathcal{C}_n} \tilde{M}_n) \\ &\text{subject to } \text{Tr}_3(R_{\mathcal{C}_n}) = \frac{\mathbb{1}_2}{d} \otimes R_{\mathcal{C}_n}^{(1)}, \\ &\text{Tr}_1(R_{\mathcal{C}_n}^{(1)}) = \frac{\mathbb{1}_0}{d}, \\ &R_{\mathcal{C}_n} \geq 0, \quad R_{\mathcal{C}_n}^{(1)} \geq 0. \end{aligned} \quad (57)$$

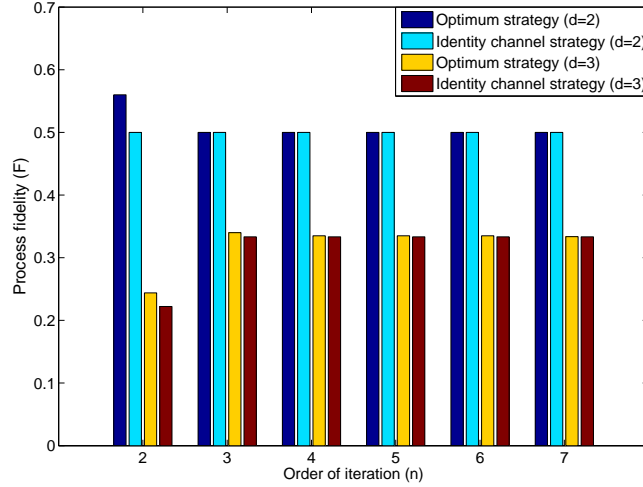


FIG. 6. The optimum fidelity in approximating  $\text{Iter}_n$ .

This is an example of Semidefinite Programming (SDP) [30], which is numerically solvable using packages like CVX [31]. The optimum fidelity obtained by this method and fidelity of the identity channel are shown for different cases in Fig. 6. For  $d = 2$ ,  $n > 2$ , the identity and direct channels discussed in Sec. VI achieve the optimum fidelity, and this is quite unanticipated, since both are trivial methods where resources like entanglement or general preprocessing or postprocessing units are not used.

As in the case of other approximating processes investigated earlier, the optimum fidelity reaches a constant value, and the optimal iterator has the same performance for high enough orders  $n$ . This phenomena is not observed in the case of 1-to- $n$  cloning of unitary gates where the fidelity seems to decrease monotonically with growth of  $n$  [5]. In addition, in that problem, the performance of the optimal cloner depends crucially on the entanglement of input states with the ancillary system, and the identity channel has a by-far-worse fidelity than the optimal cloner.

## VIII. CONCLUSION

We have shown that it is impossible to iterate an unknown quantum gate by using it once, what we called it the no-iteration theorem. We have also investigated different schemes to approximately bypass this no-go result: (1) The random guess strategy in which iterations of a randomly chosen gate is performed. (2) The measure-and-prepare method where the given gate  $\mathcal{U}$  is first estimated using the state  $|U\rangle$ , and then unitary processes are performed on the input state accordingly. (3) Approximating with the identity channel or by performing the given unitary process directly on the input system. In addition, by using the notion of quantum comb, we have been able to state the problem of finding the optimal iterator as a semidefinite programming, which we have solved numerically for  $d = 2, 3$ .

The iteration problem has some unique features that make it different from similar problems like cloning of unitary channels. One is that the performance of all discussed methods including the optimal one, remains the same for highly enough orders  $n$ . In the case of random guess, we saw the connection of this phase transition to the joint distribution of eigenvalues of a random unitary matrix, which changes from being highly ordered to having no structure for  $n \geq d$ . The other feature is that the performance of trivial processes like identity or direct channels is comparable to the optimal strategies, and at least for  $d = 2, 3$ , numerical solutions show they achieve the optimum performance for  $n > d$ .

This no-go theorem is another example of transformations of quantum channels that cannot be realized perfectly. Providing these examples helps us to understand the characteristics of quantum operations as *carriers of information*, and shows us how laws of quantum mechanics act when evolution of operations is considered instead of states.

Interesting behaviors of gate iterators discussed in this paper, motivates a more general study of powers of unitary operators in  $n \gg 1$  limit. The iteration problem and the performance of the optimal iterator might also be explored when multiple copies of the oracle is provided.

## Appendix A: Alternate Proof of Theorem 1

**Alternate proof.** According to the following lemma, proved as a theorem in [32], there exists a lower bound on the performance of quantum search algorithms. This lower bound is only a few percent smaller than the number of iterations required by Grover's algorithm [12].

**Lemma A.1.** *Let  $T$  be any set of  $N$  strings, and  $M$  be any oracle quantum machine with bounded error probability. Let  $y \in_R T$  be a randomly and uniformly chosen element from  $T$ . Put  $\mathcal{O}$  to be the oracle where  $\mathcal{O}(x) = 1$  if and only if  $x = y$ . Then the expected number of times  $M$  must query  $\mathcal{O}$  in order to determine  $y$  with probability at least  $\frac{1}{2}$  is at least  $\lfloor \sin(\frac{\pi}{8})\sqrt{N} \rfloor$ .*

Now imagine that  $\text{Iter}_n$  can be constructed perfectly, then for an appropriate number of strings  $N$ , the required number of queries can be reduced. This can be done easily by replacing each  $n$  successive queries in Grover search algorithm with a single use of  $\text{Iter}_n$ . Thus, the lower bound of the last Lemma is violated and this is a contradiction.  $\square$

- 
- [1] W. K. Wootters, and W. H. Zurek, *A single quantum cannot be cloned*, Nature 299, 802 - 803(1982)
  - [2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Duek, N. Ltkenhaus, and M. Peev, *The security of practical quantum key distribution*, Rev. Mod. Phys. 81, 1301 (2009)
  - [3] M. Hillery, V. Buék, and A. Berthiaume, *Quantum secret sharing*, Phys. Rev. A 59, 1829 (1999)
  - [4] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, *Mixed-state entanglement and quantum error correction*, Phys. Rev. A 54, 3824 (1996)
  - [5] G. Chiribella, G. M. D'Ariano, and P. Perinotti, *Optimal Cloning of Unitary Transformation*, Phys. Rev. Lett. 101, 180504 (2008)
  - [6] G. Chiribella, G. Mauro D'Ariano, P. Perinotti, and B. Valiron, *Quantum computations without definite causal structure*, Phys. Rev. A 88, 022318 (2013)
  - [7] M. Arajo, F. Costa, and C. Brukner, *Computational advantage from quantum-controlled ordering of gates*, Phys. Rev. Lett. 113, 250402 (2014)
  - [8] M. Arajo, A. Feix, F. Costa, and C. Brukner, *Quantum circuits cannot control unknown operations*, New J. Phys. 16 093026 (2014)
  - [9] N. Friis, V. Dunjko, W. Dr, and H. J. Briegel, *Implementing quantum control for unknown subroutines*, Phys. Rev. A 89, 030303(R) (2014)
  - [10] A. Bisio, M. Dall'Arno, P. Perinotti, *The quantum conditional statement*, Preprint: arXiv:1509.01062 (2015)
  - [11] M. A. Nielsen, and I. L. Chuang, *Programmable quantum gate arrays*, Phys. Rev. Lett. 79, 321 (1997)
  - [12] L. K. Grover, *A fast quantum mechanical algorithm for database search*, Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC), May 1996, pages 212-219
  - [13] N. Shenvi, J. Kempe, and K. B. Whaley, *A Quantum Random Walk Search Algorithm*, Phys. Rev. A 67, 052307 (2003)
  - [14] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, *Quantum Amplitude Amplification and Estimation*, Quantum Computation and Quantum Information, Samuel J. Lomonaco, Jr. (editor), AMS Contemporary Mathematics, 305:53-74, 2002
  - [15] B. R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, *Quantum algorithms revisited*, The Royal Society, V: 454, Issue: 1969
  - [16] Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J.Sci.Statist.Comput. 26 (1997) 1484
  - [17] G. Brassard, P. Hoyer, and A. Tapp, *Quantum Algorithm for the Collision Problem*, The Royal Society, V: 454 Issue: 1969
  - [18] Ch. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, *Strengths and Weaknesses of Quantum Computing*, SIAM J. Comput., 26(5), 15101523 (1997)
  - [19] M. Raginsky, *A fidelity measure for quantum channels*, Phys. Lett. A 290, 11-18 (2001)
  - [20] G. Chiribella, G. M. D'Ariano, and P. Perinotti, *Transforming quantum operations: quantum supermaps*, Europhysics Letters 83, 30004 (2008)
  - [21] G. Chiribella, G. M. D'Ariano, and P. Perinotti, *quantum circuits Architecture*, Phys. Rev. Lett. 101, 060401 (2008)
  - [22] We thank the anonymous referee for bringing to our attention this interesting question and line of research.
  - [23] J. Emerson, R. Alicki, and K. Zyczkowski, *Scalable Noise Estimation with Random Unitary Operators*, J. Opt. B: Quantum Semiclass. Opt. 7 (2005) S347-S352
  - [24] P. Diaconis, and S. Evans, *Linear Functionals of Eigenvalues of Random Matrices*, T. of the American Math. Society, V. 353, N. 7.(Jul., 2001), pp 2615-2633
  - [25] P. Diaconis, *Patterns in eigenvalues : the 70th Josiah Willard Gibbs lecture*, Bulletin (New Series) of the American Mathematics Society, Volume 40, Number 2, Pages 155178 S 0273-0979(03)00975-3
  - [26] E. M. Rains, *High powers of random elements of compact Lie groups*, Probab. Theory Related Fields, 107:219241, 1997
  - [27] A. Acin, E. Jane, and G. Vidal, *Optimal estimation of quantum dynamics*, Phys. Rev. A 64, 050302(R) (2001)
  - [28] F. Mezzadri, *How to generate random matrices from the classical compact groups*, Notices of the AMS, Vol. 54 (2007), 592-604

- [29] A. Bisio, G. Chiribella, G. M. D'Ariano, P. Perinotti, *Minimal computational-space implementation of multi-round quantum protocols*, Phys. Rev. A 83, 022325 (2011)
- [30] L. Vandenberghe, and S. Boyd, *Semidefinite programming*, SIAM Review, Vol. 38, NO. 1. (Mar., 1996), pp. 49-95.
- [31] M. Grant, and S. Boyd, *CVX: Matlab software for disciplined convex programming*, version 2.0 beta. <http://cvxr.com/cvx>, September 2013.
- [32] M. Boyer, G. Brassard, P. Hoeyer, and A. Tapp, *Tight bounds on quantum searching*, Fortsch.Phys.46:493-506,1998